# Network security policy in Wireless networks

Amroush, Fadi
University of Aleppo, Universidad de Granada

27. November 2010

# إعداد السياسات الأمنية في الشبكات اللاسلكية

# Network security policy in Wireless networks

---


## ABTRACT

Wireless networks are spreading everywhere nowadays, So there is a need to study the security issues for it , towards a full security policy for wireless networks.

In this paper we will explain security issues for wireless networks, and how to write a network policy, its components, structure, and site survey.

The paper summarize by introducing the most ten famous risks in wireless security and how to avoid it.

عداد: م. فادي عمروش
ماجستير في هندسة الحاسبات – جامعة حلب.
ورقة عمل مقدمة للندوة الندوة العلمية " أمن الشبكات الحاسوبية ".

## الملخص Abstract

رافق انتشار الشبكات اللاسلكية شيئاً فشيئاً ظهور الحاجة لفهم أمن المعلومات ضمن الشبكات اللاسلكية، وصولاً لكتابة سياسة أمنية فعالة للشبكة اللاسلكية.

نقترح في هذه الورقة سبل تحقيق الأمن في الشبكات اللاسلكية وصولاً لكتابة دراسة أمنية واقعية للشبكات اللاسلكية، ودراسة طرق كتابة السياسات الأمنية الخاصة بالشبكات اللاسلكية.

تتحدث الورقة عن أسس أمن المعلومات، و أسس كتابة السياسة الأمنية ومكوناتها، ومن ثم تقترح الورقة كيفية تطبيق المفاهيم السابقة ضمن الشبكات اللاسلكية عن طريق استخدام طرق المسح survey للمواقع اللاسلكية، وشرح المفاهيم التقننية لكيفية تحقيق أمن المعلومات في الشبكات اللاسلكية، وصولاً بأن تتوج بتقديم المخاطر الأمنية العشر الأكثر شيوعاً في الشبكات اللاسلكية مع مجموعةً من المقترحات لكل منها.

## 1. مقدمة:

في الماضي كانت الحواسب مستقلة عن بعضها البعض وكان يتم وضعها في مراكز كبيرة تدعى مراكز معلومات، وكان يتم حماية هذه المركز من هجمات العالم الخارجي بواسطة قفل الأبواب، ومع انتشار الشبكات انتشاراً واسعاً، أصبح إغلاق الأبواب ووضع الأقفال غير كافياً لحماية الحاسب ومعلوماته من الاختراق، لأن الهجمات ستأتي الآن من الشبكة أي من أي حاسب آخر، وقد يكون حتى من دولة أخرى.

إن تحقيق الأمن لشبكة خاصة في ظل انتشار وتوسع الانترنت أمر صعب وخاصة أن الانترنت الآن تعج بالمواقع وخاصة مواقع الهاكرز وأدواتهم بشكل مجاني.

لا بغفل أحد عن أهمية تحقيق الأمن، وخاصة في مجال الشبكات وهي من الخطوات الهامة في حماية الشبكة أو بشكل أكبر أو أعم (الشركة، مركز، .....)، من هنا تأتي أهمية وجود سياسة أمنية للشبكة اللاسلكية حيث تتألف من مجموعة من اللوائح أو القواعد التي تزود المستخدمين بالقوانين والتصرفات للأعمال المسموحة والملائمة ضمن هذه الشبكة (الشركة)، وما هي الأشياء والأعمال الغير مسموح بها.

مع انتشار الشبكات اللاسلكية شيئا فشيئا برزت الحاجة لفهم أمن المعلومات ضمن الشبكات اللاسلكية وصولا لكتابة سياسة أمنية فعالة للشبكة اللاسلكية.

يعتمد تعريف الأمن إلى حد كبير على السياق، لأن كلمة الأمن تشير إلى طيف واسع من المجالات ضمن وخارج حقل تقنية المعلومات. قد نتكلم مثلاً عن الأمن عند توصيف الإجراءات الوقائية على الطرق العامة أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات. لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن، بناء على ذلك فقد قمنا بصياغة مصطلح "أمن الشبكات اللاسلكية" ضمن تصنيف محدد للأمن بغية تسهيل مهمتنا في دراسة الأمن في مجال الشبكات اللاسلكية.

## 2. أمن المعلومات.

لكي نتمكن من استيعاب مفهوم أمن المعلومات لا بد من استعراض السياق التاريخي لتطور هذا المفهوم. لقد ظل هذا المجال من الأمن حتى أو اخر السبعينيات معروفاً باسم أمن الاتصالات (Communication Security COMSEC) والذي حددته توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة بما يلي: "المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات".

تضمنت النشاطات المحددة لأمن الاتصالات COMSEC أربعة أجزاء هي: أمن التشفير Crypto security، أمن النقل Transmission Security، أمن الإشعاع Emission Security والأمن الفيزيائي Physical Security. كما تضمّن تعريف أمن الاتصالات خاصيتا: السرية والتحقق من الهوية.

**السرية:** التأكيد بأن المعلومات لم تصل لأشخاص، عمليات أو أجهزة غير مخولة بالحصول على هذه المعلومات (الحماية من إفشاء المعلومات غير المرخص).

**التحقق من الهوية:** إجراء أمني للتأكد من صلاحية الاتصال، الرسالة أو المصدر أو وسيلة للتحقق من صلاحية شخص ما لاستقبال معلومات ذات تصنيف محدد (أو التحقق من مصدر هذه المعلومات).

**التكاملية:** تعكس جودة أي نظام للمعلومات مدى صحة ووثوقية نظام التشغيل، التكامل المنطقي للتجهيزات والبرمجيات التي توفر آليات الحماية ومدى تناغم بنى المعلومات مع البيانات المخزنة.

**التوفر Availability:** الوصول الموثوق إلى البيانات وخدمات المعلومات عند الحاجة إليها من قبل الأشخاص المخولين بذلك. لاحقاً وفي التسعينات من القرن الماضي تم دمج مفهومي الأمن (أمن الاتصالات وأمن الحواسيب) لتشكيل ما أصبح يعرف باسم (أمن أنظمة المعلومات Information Systems Security – INFOSEC). يتضمن مفهوم أمن أنظمة المعلومات الخصائص الأربعة المعرفة مسبقاً ضمن مفاهيم أمن الاتصالات وأمن الحواسيب: السرية، التحقق من الهوية، الكمال والتوفر، كما أضيف إليها خاصية جديدة: مكافحة الإنكار.

**مكافحة الإنكار (المسؤولية):** التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع احتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات.

## 3. كتابة السياسة الأمنية

إن السياسة الأمنية هي اللوائح أو القواعد التي تزود المستخدمين بالقوانين والتصرفات للأعمال المسموحة والملائمة ضمن هذه الشبكة (الشركة)، وما هي الأشياء والأعمال الغير مسموح بها، هذا هو السبب الرئيسي لاستخدام اللوائح ومناهج الأمان، كما أن هناك أسباب أخرى إضافية تعرفنا أكثر بفائدة قواعد الأمان:

- ❖ تحدد التصرف الملائم والإجراءات اللازمة.
- ❖ يتم ضبط التوقعات من الإجراءات التي تتم على الشبكة.
- ❖ هذه الأهداف تعطي إمكانية العمل الجماعي سواء أكان إدارياُ أو مهنياً.
- ❖ تعرف أدوار ومسؤوليات كل مجموعة من مجموعات العمل في الشركة في حماية الشبكة.
- ❖ تقدم المساعدة في متابعة الأعمال القانونية إذا حدث تصرف غير مقبول.
- ❖ إعطاء تعاريف واضحة للمفاهيم والأفكار الأساسية لحماية الشبكة.

إن وجود قواعد وأسس أمان واضحة سوف يعطي لجميع سواء كانوا على الشبكة أو الشركة فهم واضح ومعرفة واضحة عن مسؤولياتهم ودور كل واحد منهم في حماية الشبكة (من المسؤول عن ماذا؟)، ويساعد في ضبط القواعد والعمليات في كل قسم من أقسام الشركة.

إن أول خطوة في كتابة أي سياسة أمنية هو تحليل المخاطر ودراستها، إن تحليل المخاطر يعني دراسة ماذا تريد أن تحمي ضمن شبكتك ومن ماذا تريد حمايته وكيف ستتم حمايته، وهذا يعني تحديد المخاطر ووضعها ضمن مستويات ودرجات وطرق تجنبها ومواجهتها عند حدوثها .

### 1.3. أسس أي سياسة أمنية :

كلنا يعلم أن كتابة سياسة أمن للشبكات لها خصوصيتها ولكن لا يخلو الأمر من بعض الأساسيات التي لا بد أن تشترك بها كل سياسة أمنية بغض النظر كانت السياسة تهدف لحماية المعلومات أو حماية الشبكات.

**الحماية الفيزيائية :**هناك تداخل كبير بين حماية الشبكة والحماية الفيزيائية لان هيكلية شبكة مؤسسة ما قد تمتد لتشمل بناء كامل، مدينة ، دولة وحتى العالم كله وعليه فإننا نحتاج لحماية فيزيائية لمحتويات الشبكة الفيزيائية من كابلات وموجهات ...الخ وبدون الحماية الفيزيائية لن يكون هناك أي معنى للكلام عن مبادئ سرية الشبكات مثل التكاملية والموثوقية .عندما نتحدث عن الحماية الفيزيائية هذا يعني أن نكتب ونوجد طرق حماية الموارد الفيزيائية من قطع هاردوير وتحديد الأشخاص المسؤولين عن الحماية والأشخاص المسؤولين عن منح السماحيات للأشخاص الذين يدخلون غرف السيرفر وغرف تمديد الأسلاك .

**حماية الشبكة:**تعنى حماية الشبكة بحماية تمديدات الشبكة وأسلاكها ويشمل هذا القسم وجود أدوات قياس ومراقبة للوصول ومثل على تلك الأدوات وجود جدار ناري، مراقبة الشبكة، تقييد خدمات مثل الوصول عن بعد ، خدمات مشاركة الملفات، خدمات الانترنت .

**التحكم بالوصول:** يهتم هذا القسم بتحديد هو ية من يدخل الشبكة وإلى أين يدخل وما هو سبب دخوله ويجب أن توجد إجرائية واضحة للتأكد من أن الأشخاص الحقيقيين هم الذين يمتلكون حق الوصول للخدمات والمعلومات الخاصة بهم دون غيرهم وبالتالي يجب أن تكون السياسة قادرة على منح المديرين المرونة الكافية لمنح الصلاحيات للمستخدمين والتحكم بها منعا لحدوث أخطاء .

**التأكد من الهوية:** يعنى التأكد من الهوية بكيفية اختبار المستخدمين فيما إذا أنهم فعلا المستخدمين الحقيقيين ، إن طرق التحقق من الهوية تتراوح من وجود رقم معرف وكلمة سر خاصة بكل مستخدم، إلى طرق التأكد التي تعتمد على معدات صلبة، مثل التأكد عن طريق بطاقات ممغنطة أو التأكد من البصمة، وحدقة العين وطبعاً يتراوح استخدام هذه التقنيات حسب الأهمية والحاجة .

**التشفير:** يعتبر التشفير أحد الأمور الهامة لتحقيق تكامل المعطيات ويقصد بتكامل المعطيات حماية المعطيات المرسلة عبر الشبكة ومن التعديل والتزوير وغالباً ما يكون التشفير ضروريا عندما يتم نقل المعلومات لمستخدمين بعيدين أو عند دخول أحد المستخدمين عن بعد لجهاز ما وخاصة في ظل وجود شبكة انترانت

**المراقبة والمراجعة:** ما إن تقوم بوضع سياستك الأمنية لشبكتك وتنفذها عليك بعد فترة التأكد من أن المكونات والموظفون يطبقون ويلتزمون هذه السياسة، ويتم ذلك بمراقبة تطبيق هذه السياسة، تفيد السياسة في التعـــرف على المشاكل والتنبؤ بها قبل حدوثها ويجب مراجعة السياسة باستمرار للتأكد من استمرار فعاليتها .

**خطة طوارئ:** يجب أن تحتوي سياستك على قسم يشرح الاجرائيات الواجب اتخاذها في حال حدوث كارثـــة وبالتالي عليك تحديد كيفية وتوقيت استرجاع البيانات عند حدوث هجوم يؤدي لضررها وتحديد كيفيـــة صـــد هجوم وكيفية حفظ النسخ الاحتياطية ومكانها والمسؤولون عليها .

**السياسة الشخصية:** يحدد هذا القسم السياسة الشخصية لكل مستخدم لديك على الشبكة وما هـــي الســـماحيات التي يملكها على موارد الشبكة مثل الطابعة والانترنت ويجب تحديد السماحيات بدقة مثل سماحيات اســـتخدام الألعاب، استخدام البريد الالكتروني، تصفح الانترنت واستخدام ما سبق للفائدة الشخصية

**سرية البرامج:** يجب تحديد نوعية البرامج التي تم تنزيلها على السيرفر وهل هي تجارية أو غير تجاريـــة ، موثوقة أم غير موثوقة بالإضافة لتقييد تحميل البرامج من الانترنت وتنصيبها على السيرفر مباشرة.

### 2.3. خطوات كتابة سياسة أمنية :

**تحديد الهدف Objective** : قبل الشروع بكتابة سياستك الأمنية يجب أن يكون لديك فكرة واضحة عن أهداف هذه السياسة.

**المدى Scope:** وهو ما ستقوم بحمايته بواسطة سياستك الأمنية ، وهذا يشمل ذكر كل المجالات اللازمة للحماية انطلاقاً من الحماية الفيزيائية حتى الشخصية و مدى شمولية هذه السياسة من مدراء و مستخدمين و حتى الزوار.

**المناقشة و دعم الادارة العليا:** بعد كتابة الهدف و أفق السياسة يجب إطلاع الادارة العليا في مؤسستك عليها وأخذ الموافقة و النقاش معهم حول طرق تحقيق هذه السياسة.

**الاطلاع على سياسات أخرى:** ينصح قبل الشروع بكتابة السياسة الأمنية الخاصة بك أن تطلع على سياسات عامة لشركات أخرى و تجارب الشركات الأخرى في هذا المجال.

**تقدير المخاطر:** قبل كتابة السياسة يجب عليك تحديد المخاطر المتوقعة و طرق مواجهتها، حيث تحديد مكونات السياسة و كتابتها يعتمد ذلك على دراسة المخاطرة إذ ليس من الضروري وضع كل المكونات السابقة عند كتابة سياسة أمنية،ويعتمد ذلك على تقديرك للمخاطر المتوقعة ومقدار سرية المعلومات التي تتضمنها شبكتك، فالشبكة في المقهى الإلكتروني تختلف عن تلك في امتحانات الجامعة بالتأكيد.

**التقييم:** بعد أن تكتب السياسة عليك القيام بتقييمها ،و تساعدك الأسئلة التالية في تقييم سياستك:

- هل تتوافق سياستك مع القانون.

- هل تقيد نفوذ موظفيك .
- هل هي قابلة للتطبيق العملي.
- هل تعرف كل الأشكال المختلفة للاتصالات.

### 3.3. مثال عن قواعد الأمان عند إنشاء كلمة المرور:

هذا المثال يعطي تطبيقاً عن قواعد الأمان المتبعة والشروط المطلوب توضيحها عند استعمال أو إنشاء كلمة مرور. إن الهدف أو الغاية من هذا المنهج هو ترسيخ معيار قياسي لإنشاء كلمات مرور قوية وحماية كلمات المرور الموجودة وتحديد الفترة الزمنية الفاصلة قبل أن يصبح من الضروري تغيير هذه الكلمة.

يتضمن هذا النهج توصيف لكل الأشخاص الذين يجب أن يلتزموا به، وفعلياً هم جميع الموظفين سواءً كانوا ذوي المواقع الهامة والحساسة أو حتى غير الحساسة وكذلك العاملين في أي نظام يتواجد في أي فرع من فروع الشبكة أو الذي له وصول إلى شبكة الشركة أو الذي يخزن المعلومات غير العامة للشبكة.

**القواعد العامة**

- ❖ كل كلمات المرور التي على مستوى النظام يجب أن تكون جزءً من قاعدة بيانات إدارة كلمات المرور العمومية والتي يكون مسؤول عنها فريق أمان الشبكة.
- ❖ كل كلمات المرور التي على مستوى المستخدم يجب تغييرها كل 6 أشهر على الأقل.
- ❖ لا يجب إدراج كلمات المرور في رسائل البريد الالكتروني أو في بقية أشكال الاتصالات الالكترونية.
- ❖ لا يجب إنشاء كلمة المرور لأحد أبداً ويجب إبلاغ المسؤولين عن أمان الشبكة في حال طلب شخص ما التعرف على كلمة المرور.

**إرشادات عامة عن ترشيد كلمة المرور:**

إن كلمة المرور تعتبر من أنظمة الحماية الأولية أي هي خط نظام الدفاع الأول لدى المستخدم وبالتالي فإن تحديد نقاط الضعف عند اختيار كلمة المرور أو تحديد الأسلوب الأفضل لذلك، لذلك تعتبر من الخطوات الهامة في أمن وحماية الشبكات (المعلومات). لذلك سنقوم بتوضيح بعض النقاط.

**ميزات كلمات المرور الضعيفة**

- ❖ تحتوي كلمة المرور على أقل من 8 أحرف.
- ❖ كلمة المرور هي كلمة موجودة في القاموس.
- ❖ كلمة المرور هي كلمة شائعة الاستعمال (أسماء فرق رياضية، مسرحية، ممثلون، مواليد، أصحاب، الأب، الأم،.....).

- ❖ نفس الخطوات السابقة يسبقها عدد أو يليها عدد.

**ميزات كلمات المرور القوية**

- ❖ تحتوي على أحرف كبيرة وصغيرة.
- ❖ فيها أعداد وأحرف ورموز وأقواس.
- ❖ أقل طول لها 8 أحرف رقمية أو أبجدية أو كلاهما.
- ❖ ليست كلمات في أي لغة أو لهجة أو كلمات شائعة.
- ❖ لا ترتبط بأي معلومات شخصية أو عائلية أو عاطفية.
- ❖ عدم تخزين هذه الكلمات على ورقة أو إلكترونياً.
- ❖ يجب انتقاء كلمات سهلة الحفظ بالنسبة للشخص أو المستخدم.

## 4. مسح الموقع اللاسلكي Site survey

إن أول خطوة قبل كتابة السياسة الأمنية لشبكة لاسلكية هو القيام بعملية مسح للموقع المراد تنفيذ شبكة لاسلكية ضمنه، وهو ما يسمى Wireless Site Survey وستكون دراسة الحالة للمسح اللاسلكي وهو الطابق الأول ضمن مؤسسة البريد بحلب، حيث تفترض الحالة تنفيذ أمن شبكة لاسلكية في الطابق المذكور. إن تنفيذ عملية المسح تتم بالإجابة على استبيان معين لتنفيذ المسح.

| **معلومات الاتصال** | |
|---|---|
| اسم الموقع | |
| عنوان الموقع | |
| اسم الشخص المسؤول | |
| رقم الهاتف | |
| **معلومات الموقع** | |
| قم بوصف الموقع – التجهيزات الحالية | |
| صف موقع نقطة الولوج المحتملة | |
| أين سيتم تركيب نقطة الولوج | السقف – الحائط – الرف |
| هل يوجد نقطة شبكة قرب نقطة الولوج – كم تبعد . | |
| هل يوجد نقطة كهرباء قرب نقطة الولوج – كم تبعد . | |
| هل يمكن الوصول لنقطة الوصول من العامة | |
| هل ستتم حماية نقطة الولوج فيزيائيا- كيف | |
| صف أي معلومات مفيدة حول الموقع واستخدام الشبكة اللاسلكية والامن المطلوب | |

جدول 1 استبيان مسح فارغ

بالإجابة على الاستبيان نحصل على تصور عام للسياسة الأمنية الواجب كتابتها وفق حاجات المستخدم ووضع الشبكة الحالي ، يوضح الجدول التالي الإجابات على الاستبيان السابق ضمن مؤسسة البريد بحلب الحالة المفترضة:

| معلومات الاتصال | |
|---|---|
| **اسم الموقع** | الطابق الأول في المبنى |
| **عنوان الموقع** | مؤسسة البريد بحلب |
| **اسم الشخص المسؤول** | أحمد الصالح |
| **رقم الهاتف** | **2252112** |
| **معلومات الموقع** | |
| **قم بوصف الموقع – التجهيزات الحالية** | |
| يقع الموقع في الطابق الأول – يوجد شبكة حالية ممددة ضمن الطابق وموصولة مع الانترنت. | |
| **صف موقع نقطة الولوج المحتملة** | |
| يجب أن يكون الموقع ضمن الطابق بحيث يغطيه كله وبما أنه شبه دائري سنوزع ثلاث نقاط وصول ضمن الطابق. | |
| **أين سيتم تركيب نقطة الولوج** | **السقف – الحائط – الرف** |
| السقف بشكل أفقي لتحقيق التغطية بشكل أفقي للطابق. | |
| هل يوجد نقطة شبكة قرب نقطة الولوج – كم تبعد . | |
| نعم تبعد 10 متر | |
| **هل يوجد نقطة كهرباء قرب نقطة الولوج – كم تبعد .** | |
| نعم تبعد 10 متر | |
| **هل يمكن الوصول لنقطة الوصول من العامة** | |
| لا | |
| **هل ستتم حماية نقطة الولوج فيزيائيا- كيف** | |
| لا | |
| **صف أي معلومات مفيدة حول الموقع واستخدام الشبكة اللاسلكية والامن المطلوب** | |
| إن الشبكة مطلوبة للوصول على الانترنت ومنع غير المخولين من الوصول لموارد الشبكة | |

جدول 2 شكل استمارة مسح المواقع

### 1.4. الأسئلة المتعلقة بالسياسة الأمنية:

- **من هم شريحة مستخدمي الشبكة:** المدراء– الموظفون– المواطنون.
- **ما هو الهدف الرئيسي للشبكة:** الوصول للإنترنت لاسلكياً من قبل **الجميع** وإمكانية الدخول **للموارد عن بعد من قبل المدراء**.
- **هل الشبكة مفتوحة للجميع: نعم** يمكن للجميع الوصول للشبكة **ولكن السماحيات تختلف من شخص لآخر حسب المجموعة** التي ينتمي لها.
- **هل تريد تشفير ضمن الشبكة:** نعم نريد تشفير البيانات لمنع غير المخولين من الوصول لموارد الشبكة.
- **ما هي أنواع الأجهزة التي ستضم للشبكة:** أجهزة المحمول – الاجهزة المزودة ببطاقات شبكة لاسلكية .
- **ما هي سرعة بطاقات الشبكة اللاسلكية بشكل عام:** 54 ميغا.
- **هل هناك الحاجة لتحديد نوع المستخدمين أم لا:** لا داعي للتحديد في حالة الموظفين والمواطنين، ولكن هناك الحاجة في حالة المدراء.
- **هل سيتم دخول المستخدمين بشكل آلي للشبكة أم سيتم تخصيص ارقام أي بي لهم:** الدخول سيتم بشكل آلي، أي استخدام DHCP –لا يمكن تحديد أي مواطن سيدخل للشبكة–

- **هل هناك فترة محددة للدخول للشبكة :** نعم من 8 صباحا حتى 8 مساء.
- **هل هناك جهاز معين للإدارة:** نعم

## 5. أمن المعلومات والشبكات اللاسلكية

تعرّف توصيات أمن أنظمة المعلومات والاتصالات لوكالة الأمن القومي في الولايات المتحدة أمن أنظمة المعلومات كما يلي: "حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف، توثيق ومواجهة هذه التهديدات".

يقدم النموذج المرجعي Open Systems Interconnect OSI والذي ابتكرته منظمة المعايير الدولية ISO توصيفاً نظرياً لتصميم بروتوكولات الشبكات (الاتصالات) الحاسوبية. يقوم هذا النموذج بتقسيم وظائف الاتصال المختلفة إلى سبعة طبقات مختلفة تعمل بشكل مستقل عن بعضها البعض.

يتبع تصميم البروتوكولات وفق نموذج OSI مبدأ "التكديس Stack". إن استخدام نموذج للبروتوكولات يعمل وفق مبدأ الطبقات أو التكديس يعني أن كل طبقة ستستخدم وظائف الطبقة الأدنى منها فقط في حين تقوم بتخديم الطبقة التي تعلوها مباشرة فقط. ينعكس أسلوب التصميم وفق مبدأ الطبقات بشكل مباشر على كيفية تطبيق الخصائص الأمنية.

### 1.5. السرية في الشبكات اللاسلكية:

يشكل التشفير على مستوى الوصلة آليةً لتأمين البيانات أثناء انتقالها بين نقطتين متصلتين بنفس الوصلة الفيزيائية (ويمكن أيضاً أن يتصلا عبر وصلتين فيزيائيتين مربوطتين بمكرر للإشارة كما هو الحال في وصلات الأقمار الصناعية). يتيح التشفير على مستوى الوصلة حماية البروتوكولات أو البيانات المارة عبر الوصلة الفيزيائية من أعين المتطفلين.

يتطلب التشفير توفر مفتاح محدد أو سر مشترك بين الأطراف التي ستشترك في عملية التشفير بالإضافة إلى الاتفاق عل خوارزمية مشتركة للتشفير. في حال عدم تشارك المرسل والمستقبل في نفس الناقل الفيزيائي ينبغي فك تشفير البيانات وإعادة تشفيرها عند كل نقطة مرور أثناء انتقالها إلى المستقبل. يستخدم التشفير على مستوى الوصلة عادة عند غياب التشفير على مستويات أعلى.

لقد ارتبط مفهوم سرية الشبكة اللاسلكية بمصطلح "السرية المكافئة للشبكة السلكية WEP". وقد شكلت WEP جزءاً من المعيار الأساسي IEEE 802.11 للشبكات اللاسلكية في العام 1999.

إن الهدف الرئيس من السرية المكافئة للشبكة السلكية WEP هو تأمين الشبكات اللاسلكية بمستوى من السرية مماثل للسرية المتوفرة في الشبكات السلكية. إن الحاجة إلى هذا البروتوكول كانت جلية: فالشبكات اللاسلكية تستخدم الأمواج اللاسلكية وبالتالي فهي أكثر عرضةً لأعين المتطفلين.

لقد كان عمر بروتوكول السرية المكافئة للشبكة السلكية WEP قصيراً للغاية، فقد أدى تصميمه الرديء وغير الشفاف إلى نجاح العديد من الهجمات في اختراق الشبكات التي تستعمل هذا البروتوكول. لم يستغرق الأمر سوى عدة أشهر من إطلاق البروتوكول حتى تم خرقه وهجرانه. على الرغم من أن طول مفاتيح التشفير كان محدوداً نتيجة بعض قوانين حظر التصدير إلا أن هذا البروتوكول قد أثبت ضعفه بغض النظر عن طول مفتاح التشفير المستخدم، لكن العيوب التصميمية لم تكن السبب الوحيد في فشل بروتوكول السرية المكافئة للشبكة السلكية WEP، بل أن عدم توفر نظام لإدارة مفاتيح التشفير ضمن نفس البروتوكول قد ساهم أيضاً في إفشاله. لم يتضمن بروتوكول السرية المكافئة للشبكة السلكية WEP أي نظام لإدارة مفاتيح التشفير على الإطلاق، وكانت الوسيلة الوحيدة لتوزيع مفاتيح التشفير تتطلب إعداد / إدخال هذه المفاتيح يدوياً في كل وحدة من التجهيزات اللاسلكية (إلا أن السر المشترك بين عدة أشخاص لم يعد سراً!).

بعد موت بروتوكول السرية المكافئة للشبكة السلكية WEP تم اقتراح بروتوكول الوصول المحمي للشبكة اللاسلكية WPA في العام 2003 ليتم اعتماده فيما بعد كجزء من معيار الشبكات اللاسلكية IEEE 802.11i عام 2004 تحت اسم WPA2. لقد تم تصميم بروتوكولي WPA وWPA2 للعمل مع أو دون وجود مخدم لإدارة مفاتيح التشفير. في حال غياب مخدم إدارة مفاتيح التشفير فإن جميع المحطات ستستخدم "مفتاح تشفير مشترك مسبقاً (Pre-Shared Key" (PSK). يعرف هذا النمط من التشغيل باسم بروتوكول WPA أو WPA2 الشخصي.

يعرف بروتوكول WPA2 عند استخدام مخدم لمفاتيح التشفير ببروتوكول WPA المؤسساتي. يتطلب بروتوكول WPA2 المؤسساتي وجود مخدم يعمل بمعايير IEEE 802.1X لتوزيع مفاتيح التشفير. من أهم التطويرات المضمنة في بروتوكول WPA2 مقارنة بسلفه WEP هو إمكانية تبادل مفاتيح التشفير ديناميكياً بواسطة بروتوكول تكامل مفاتيح التشفير المؤقتة (Temporal Key Integrity Protocol (TKIP.

## 2.5. التحقق من الهوية في الشبكات اللاسلكية

يتم تعريف التحقق من الهوية في سياق الشبكات اللاسلكية بالإجراءات الهادفة لضمان صلاحية الاتصال بين نقاط الولوج و/أو المحطات اللاسلكية. يمكن التعبير عن التحقق من الهوية في الشبكات اللاسلكية بشكل أبسط باعتباره حق إرسال البيانات إلى وعبر الشبكة اللاسلكية.

### إيقاف إرسال معرف مجموعة الخدمات SSID كإجراء لتعزيز أمن الشبكة اللاسلكية

إن إيقاف إرسال معرف مجموعة الخدمات SSID يعني ضمنياً بأن على مستخدمي الشبكة اللاسلكية الحصول مقدماً على معرّف مجموعة الخدمات الذي يجب استخدامه للربط مع نقطة ولوج (أو مجموعة من نقاط الولوج). لقد تم استخدام هذه الميزة الجديدة من قبل الكثير من مصنعي تجهيزات الشبكات اللاسلكية كإجراء لتعزيز أمن الشبكة. في واقع الأمر فإنه وعلى الرغم من أن إيقاف إرسال معرف مجموعة الخدمات سيمنع المستخدمين غير المخولين من الحصول على هذا المعرف عبر الإطار المرشد، إلا أنها لن تمنع إيجاد معرّف مجموعة الخدمات باستخدام برمجيات التجسس على إطارات الربط المرسلة من محطات أخرى. إن

إيجاد معرف مجموعة الخدمات لشبكة مغلقة يعني ببساطة انتظار أحد ما ليقوم بالربط بالشبكة اللاسلكية واستخلاص معرّف مجموعة الخدمات من إطار الربط المرسل.

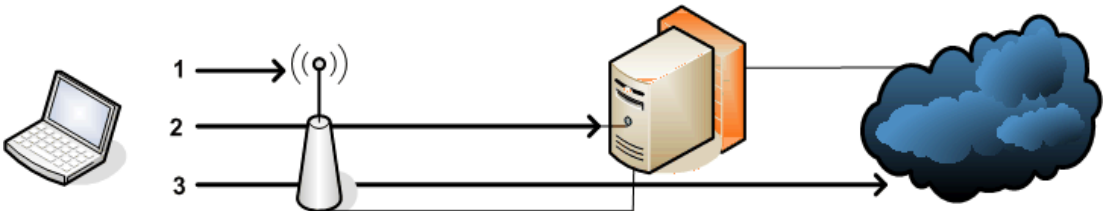
**استخدام فلترة العناوين الفيزيائية MAC كإجراء لتعزيز أمن الشبكة اللاسلكية**

لقد انتشر استخدام العنوان الفيزيائي لبطاقة الشبكة اللاسلكية كآلية لتحديد أو توفير الوصول إلى الشبكة اللاسلكية بين الكثير من مزودي خدمات الإنترنت اللاسلكية. يعتمد هذا الخيار على اعتبار أن العناوين الفيزيائية MAC مسجلة ضمن المكونات الإلكترونية لبطاقة الشبكة وبالتالي يستحيل تغييرها من قبل المستخدمين العاديين. إلا أن الواقع يخالف هذا الاعتبار، لأنه من الممكن وببساطة تغيير العناوين الفيزيائية في معظم بطاقات الشبكة اللاسلكية.

**البوابات المقيّدة للشبكات اللاسلكية**

عند استخدام البوابات المقيدة كآلية للتحقق من الهوية في شبكةٍ ما فإن مستخدمي هذه الشبكة سيتمكنون من الربط مع أية نقطة ولوج (دون استخدام آليات التحقق من الهوية في الشبكة اللاسلكية) والحصول على عنوان إنترنت IP عبر بروتوكول الإعداد التلقائي للمضيف DHCP، بعد حصول المستخدم على عنوان إنترنت IP ستقوم الشبكة بالتقاط جميع طلبات الوصول إلى الإنترنت عبر بروتوكول HTTP لإجبار المستخدم على "تسجيل الدخول" إلى صفحة إنترنت.

تضطلع البوابات المقيّدة بمهمة التأكد من صحة كلمة السر التي أدخلها المستخدم وتعديل حالة الجدار الناري. تعتمد قواعد الجدار الناري على قيم العنوان الفيزيائي MAC وعنوان الإنترنت IP الذي حصل عليه المستخدم عبر بروتوكول DHCP.




الشكل 1: بوابة مقيّدة مع الخطوات الثلاث للتحقق من الهوية

يظهر الشكل السابق الخطوات الثلاث لعملية التحقق من الهوية باستخدام البوابات المقيّدة. تتطلب الخطوة الأولى أن يتم ربط المستخدم مع الشبكة اللاسلكية. لا تتطلب هذه المرحلة التحقق من هوية المستخدم عبر بروتوكولات WEP/WPA وتقوم الشبكة عادةً بإرسال معرّف مجموعة الخدمات SSID. في الخطوة الثانية يحصل المستخدم على عنوان إنترنت IP عبر بروتوكول الإعداد التلقائي للمضيف DHCP. تقوم نقطة الولوج بتمرير سيل البيانات IP دون أي تحقق من هوية المستخدم. في الخطوة الثالثة والأخيرة يتم تحويل جميع طلبات الوصول إلى الشبكة عبر بروتوكول الربط التشعبي HTTP الواردة من الزبون إلى

مخدم البوابة المقيّدة. يقوم المستخدم بتسجيل الدخول إلى المخدم، أخيراً يقوم مخدم البوابة المقيّدة بتعـديل أو إضافة قاعدة ضمن الجدار الناري للسماح للمستخدم بالوصول إلى الإنترنت.

### 3.5. تكاملية البيانات في الشبكات اللاسلكية

سنقوم بتعريف كمال البيانات في الشبكات اللاسلكية بقدرة بروتوكول الاتصال اللاسلكي على كشف أي تحريف في البيانات المنقولة من قبل أشخاص غير مخولين. حلّت بروتوكولات WPA وWPA2 مشكلة كمال البيانات الموجودة في سلفها WEP بإضافة شيفرةٍ أكثر أمناً للتحقق من الرسالة إضـافةً إلـى عـدادٍ للإطارات والذي يمنع ما يسمى بـ "هجمات الإعادة Replay Attacks" التي يقوم فيها المهاجم بتسـجيل المحادثة بين أحد مستخدمي الشبكة اللاسلكية ونقطة الولوج بغية الحصول على وصول غير مخول إلى هـذه الشبكة. بإعادة المحادثة "القديمة" لن يحتاج المهاجم إلى معرفة السر المشترك لـ WEP أو المفتاح.

### 4.5. توفر الشبكات اللاسلكية

هي القدرة التقنية على ضمان الوصول الموثوق إلى خدمات البيانـات والمعلومـات للمسـتخدمين المخولين، فمن أول الأمور الواجب أخذها بعين الاعتبار أنه من غير اليسير أن تمنع شخصاً ما من التشويش على إشارة شبكتك اللاسلكية. تعمل الشبكات اللاسلكية ضمن نطاقٍ محدد للقنوات الراديوية يمكن اسـتخدامه من قبل أي شخص لإرسال إشاراتٍ لاسلكيةٍ. من شبه المستحيل منع الأشخاص غير المخولين من التشـويش على شبكتك. غاية ما يمكنك عمله أن تقوم بمراقبة وصلاتك لتحديد المصادر المحتملة للتشويش. هناك العديد من الأسباب التي قد تخفض من أداء الشبكة اللاسلكية أو توقف عملها بالكامل. قد يتسبب وجود نقاطٍ مخفيـةٍ في تدنٍ كبيرٍ في الأداء، كما قد تتسبب الفيروسات، برمجيات الند للند Peer-to-Peer إضافة إلى الرسائل المرسلة عشوائياً SPAM ، وغيرها في تخفيض سعة نقل البيانات المتوفرة للوصول المخول إلى الخـدمات الأساسية.

### 5.5. مكافحة الإنكار (المسؤولية) في الشبكات اللاسلكية

لا تتعامل معايير الشبكات اللاسلكية IEEE 802.11 مع (المسؤولية) عن المعلومات المنقولة عبر الشبكة اللاسلكية. لا تحتوي بروتوكولات الشبكات اللاسلكية على آليةٍ للتأكيد على أن مرسـل البيانـات قـد حصل على إثباتٍ لتسلم المستقبل لرسالته أو على أن المستقبل قد حصل على إثباتٍ لهوية المرسل. لذلك يجب إعداد المسؤولية ضمن بروتوكولات الطبقات العليا.

## 6. التهديدات الأمنية للشبكات اللاسلكية

يظهر الجدول التالي المخاطر الأمنية العشر الأكثر شيوعاً في الشبكات اللاسلكية ويقدم مجموعة من المقترحات لكل منها.

| | | | |
|---|---|---|---|
| 1 | **السرية** | خطر التجسس، قد يصل المستخدمون غير المخولين إلى البيانات المنقولة عبر شبكتك اللاسلكية | استخدم التشفير على مستوى الوصلة ضمن وصلاتك اللاسلكية (WPA2). |
| 2 | | خطر اختطاف البيانات المنقولة، قد يتمكن المستخدمون غير المخولين من تطبيق هجمات الشخص الوسيط | راقب نسبة الإشارة إلى الضجيج SNR، معرّف مجموعة الخدمات SSID إضافة إلى العنوان الفيزيائي لنقطة الولوج AP MAC المستخدمة في وصلاتك. |
| 3 | | خطر الوصول غير المخول إلى شبكتك وإلى الإنترنت | قم بإعداد بوابة مقيدة Captive Portal. |
| 4 | **التحقق من الهوية** | خطر الوصول غير المخول إلى شبكتك اللاسلكية | لا تعتمد على أساليب التحقق من الهوية باستخدام العنوان الفيزيائي MAC فقط.<br>لا ترسل معرّف مجموعة الخدمات SSID الخاص بشبكتك. |
| 5 | **التكامل** | خطر تحريف البيانات أثناء نقلها لاسلكياً | انصح مستخدمي شبكتك باستخدام "التشفير" ضمن الطبقات ذات المستوى الأعلى (HTTPS, Secure SMTP) .<br>استخدم التشفير على مستوى الوصلة ضمن وصلاتك اللاسلكية (WPA2). |
| 6 | **التوفر** | خطر التشويش اللاسلكي<br>إيقاف عمل الخدمة بسبب التشويش اللاسلكي (التداخل) | راقب طيف الترددات اللاسلكية دورياً.<br>حاذر من الزيادة المفرطة لطاقة وصلاتك. |
| 7 | | خطر انخفاض سعة النقل نتيجة الإرسال المتكرر للإشارات اللاسلكية | تأكد من عدم وجود نقاط مخفية أو مصادر أخرى للتشويش.<br>راقب نقاط الولوج لكشف أية إرسالات متكررة على مستوى الوصلة. |
| 8 | | خطر انخفاض سعة النقل نتيجة البرمجيات المؤذية | راقب البيانات المنقولة<br>ركّب أنظمة كشف التسلل Intrusion Detection Systems إذا دعت الحاجة. |
| 9 | **التحقق من الهوية** | خطر الوصول غير المخول لشبكتك الداخلية | قم بتركيب الشبكة اللاسلكية خارج حدود الجدار الناري. |
| 10 | **الوصول إلى الشبكة** | خطر الاستخدام غير المخول لموارد الشبكة والشبكة اللاسلكية | استخدم البوابات المقيدة المعتمدة على التواقيع الإلكترونية Digital Signature. |

جدول 3 : التهديدات الأمنية العشر الأكثر شيوعاً في الشبكات اللاسلكية مع نصائح للإجراءات الوقائية

# 7. المراجع

تم أخذ فقرات حرفية لاغناء الشرح النظري من "مواد تدريبية في الشبكات اللاسلكية للدول النامية:
إعداد: برونوروجر- النسخة العربية: أنس طويلة" وهي الفقرتين الاخيرتين حول امن المعلومات و التهديدات الأمنية للشبكات اللاسلكية.

**Wireless Hacks [1]**
100 Industrial-Strength Tips & Tools
الناشر: O'REILLY
المؤلّف: روب فليكنغر
الإصدار الأو ل: أيلول 2003
ISBN: 0-596-00559-8
– يمكن الرجوع له لمزيد من المعلومات حول الفصل الثاني –الاساسيات الفيزيائية للشبكات اللاسلكية–

**802.11 Wireless Networks: The Definitive Guide [2]**
Creating and Administering Wireless Networks
الناشر: O'REILLY
المؤلّف: ماثيوغاست
الإصدار الأو ل: نيسان 2002
ISBN: 0-596-00183-5
ماثيوغاست، نيسان 2002،
– يمكن الرجوع له لمزيد من المعلومات حول الفصل السابع –كتابة سياسة أمنية–

**[3] الدليل الكامل للشبكات اللاسلكية 802.11 Wireless Networks: The Definitive Guide 802.11، الإصدار الأو ل. أو ريللي O'Reilly**
ISBN: 0-596-00183-5
– يمكن الرجوع له لمزيد من المعلومات بشكل عام حول الشبكات اللاسلكية.

**"[4]Wireless Home Networking for Dummies"**
داني بريير، بات هو رلي ووالتر بروس
الناشر: For Dummies (27 أيار 2003)
ISBN: 0764539108
– يمكن الرجوع له لمزيد من المعلومات بشكل عام حول الشبكات اللاسلكية.

**"[5]802.11 Wireless Networks: The Definitive Guide"**
بناء وإدارة الشبكات اللاسلكية
المحرر: O'Reilly
ماثيوغاست
الإصدار الأو ل: نيسان 2002
ISBN: 0-596-00183-5
– يمكن الرجوع له لمزيد من المعلومات بشكل عام حول الشبكات اللاسلكية.

**"[6]Building Wireless Community Networks"**
روب فليكينغر
176 صفحة

الناشر: O'Reilly
الإصدار الثاني: 23 حزيران 2003
ISBN: 0596005024
– يمكن الرجوع له لمزيد من المعلومات بشكل عام حول الشبكات اللاسلكية.

**[7]"Windows XP Home Networking"**
بأو ل ثوروت
480 صفحة
الناشر: Wiley
الإصدار الأو ل: 17 تموز 2002
ISBN: 0764536753
– يمكن الرجوع له لمزيد من المعلومات حول إعداد التجهيزات اللاسلكية.

http://standards.ieee.org/wireless/
موقع معهد مهندسي الكهرباء والإلكترون IEEE الخاص بمعايير الشبكات اللاسلكية. يحتوي تفاصيل عن جميع المعايير من 802.1 إلى 802.16

أمن الشبكات اللاسلكية: تاريخ موجز
ماثيوغاست. 2002.
http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html

مقدمة إلى أمن الشبكات اللاسلكية
http://www.answers.com/topic/wireless-security

WPA مقارنةً مع WPA2: جدول مقارن
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item0900aecd801e3e59.shtml